



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: **COMMISSIONER FOR PATENTS**
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/771,472	01/26/2001	Jean Louis Calvignac	RAL920000119US1	6208
25299	7590	07/26/2007		
IBM CORPORATION PO BOX 12195 DEPT YXSA, BLDG 002 RESEARCH TRIANGLE PARK, NC 27709			EXAMINER TRAN, ELLEN C	
			ART UNIT 2134	PAPER NUMBER
			MAIL DATE 07/26/2007	DELIVERY MODE PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary

Application No.

09/771,472

Applicant(s)

CALVIGNAC ET AL.

Examiner

Ellen C. Tran

Art Unit

2134

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 18 May 2007.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-20 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-20 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on _____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
- ☐ Certified copies of the priority documents have been received.
 - ☐ Certified copies of the priority documents have been received in Application No. _____.
 - ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- 1) ☒ Notice of References Cited (PTO-892)
- 2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
- 3) ☐ Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date _____.

- 4) ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____.
- 5) ☐ Notice of Informal Patent Application
- 6) ☐ Other: _____.



DETAILED ACTION

1. This action is responsive to communication: filed on 18 May 2007, with acknowledgement of an original application filed 26 January 2001.
2. A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on 18 May 2007 has been entered.
3. Claims 1-20 are currently pending in this application. Claims 1, 13, 16, and 19 have been amended. Amendments to the claims have been accepted. Claims 1, 16, and 19 are independent claims.

Response to Arguments

4. Applicant's arguments with respect to 1-20 have been considered but they are moot due to new grounds of rejection below initiated by amendment to the independent claim.

Claim Rejections - 35 USC § 102

5. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language

6. **Claims 1-4 and 9-20** are rejected under 35 U.S.C. 102(e) as being anticipated by Kaplan et al. U.S. Patent No. 6,704,871 (hereinafter '871).

As to independent claim 1, "A hardware implementation of a crypto-function comprising:" is taught in '871 col. 2, lines 16-18, note the security functions described are 'crypto-function' and the circuit is the 'hardware implementation';

"a first register storing data to be encrypted or decrypted; a second register for receiving data which has been encrypted or decrypted" is shown in '871 col. 11, lines 16-25, note the registers that facilitate bidirectional communication are interpreted to be the first register, i.e. input and second register, output;

"and combinational logic performing computation iterations of the crypto-function on data stored in the first register and outputting data to said second register in a single hardware cycle" is disclosed in '871 col. 10, lines 14-25;

"wherein the combinational logic comprises logic functions whose outputs depend solely on their inputs and utilizes logic circuits without memory" is taught in '871 col. 10, lines 26-44, note the combined operations that operate in parallel off of the same source is interpreted to be combinational logic without memory.

As to dependent claim 2, "wherein the crypto-function is a block cipher algorithm" is taught in '871 col. 10, lines 15-17.

As to dependent claim 3, "wherein the crypto-function is the Data Encryption Standard (DES) algorithm" is shown in '871 col. 10, lines 15-17.

As to dependent claim 4, "wherein the crypto-function is the CHAIN algorithm" is disclosed in '871 col. 10, lines 15-17.

As to dependent claim 10, “wherein the hardware implementation of the crypto-function uses only the combinational logic without having to store intermediate results in registers” is disclosed in ‘871 col. 10, lines 15-17.

As to dependent claim 11, wherein the hardware implementation the crypt-function computes an iterated round function in one clock cycle” is taught in ‘871 col. 10, lines 15-17.

As to dependent claim 12, “wherein the combination logic utilizes a Data Encryption Standard (DES) algorithm that is implemented in the combination logic” is shown in ‘871 col. 10, lines 15-17.

As to dependent claim 13, “wherein the combination logic utilizes logic functions whose outputs depend solely on their inputs” is disclosed in ‘871 col. 10, lines 15-44.

As to dependent claim 14, “wherein the combination logic utilizes logic circuits without memory, whereby no registers are used to store intermediate results or iterations of encipher or deciphering computations” is taught in ‘871 col. 10, lines 15-44.

As to dependent claim 15, “wherein the crypt-function is implemented in the combinational logic without intermediate registers that require loading and settling time before contents of the intermediate registers can be read” is shown in ‘871 col. 10, lines 15-44.

As to independent claim 16, “A hardware implementation of a crypto-function comprising:” is taught in ‘871 col. 2, lines 16-18

“a first register that stores data to be encrypted or decrypted; a second register that receives data which has been encrypted or decrypted” is shown in ‘871 col. 11, lines 16-25;

“and combinational logic that performs computation iteration of the crypto-function on data store in the first register and outputting data to said second register in a single hardware cycle, the combinational logic comprising logic functions whose outputs depend solely on their inputs and utilizing logic circuits without memory, wherein the crypt-function without intermediate registers that require loading and settling time before contents of the intermediate registers can be read” is disclosed in ‘871 col. 10, lines 14-44.

As to dependent claim 17, **“wherein the single hardware cycle is approximately ten clock cycles”** is disclosed in ‘871 col. 10, lines 13-25,

As to dependent claim 18, **wherein the hardware implementation of the crypto-function computes and iterated round in just one clock cycle”** is disclosed in ‘871 col. 22, lines 48-55.

As to independent claim 19, **“A hardware implementation of a crypto-function comprising:”** is taught in ‘871 col. 2, lines 16-18;

“a first register that stores data to be encrypted or decrypted; a second register that receives data which has been encrypted or decrypted” is shown in ‘871 col. 11, lines 16-25;

“and combination logic that performs computation iteration of the crypto-function on data stored in the first register and outputting data to said second register in a single hardware cycle, the combination logic comprising logic functions whose outputs depend solely on their inputs and utilizing logic circuits without memory, wherein the single hardware cycle comprises several clock cycles” is disclosed in ‘871 col. 10, lines 14-44.

As to dependent claim 20, **“wherein the cypto-function is implemented in the combination logic without intermediate registers that require loading and settling time**

Art Unit: 2134

before contents of the intermediate registers can be read” is shown in ‘871 col. 10, lines 14-44.

Claim Rejections - 35 USC § 103

7. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

8. **Claims 5-8**, are rejected under 35 U.S.C. 103(a) as being unpatentable over Kaplan et al. U.S. Patent No. 6,704,871 (hereinafter ‘871) in view of Coppersmith et al. U.S. Patent No. 6,192,129 (hereinafter ‘129).

As to **dependent claim 5**, the following is not explicitly taught in ‘871: **“wherein the combinational logic performs an invertible key-dependent round function iterated a predetermined number of times”** however ‘129 teaches “means for decrypting said encrypted data block, resulting in restoration of said plurality of input data bytes, by performing a set of inverse round functions said number of times equal to said number of rounds, wherein said set of inverse round functions comprises an inverse key-dependent substitution function which is inverse to said key-dependent substitution function, an inverse permuting function which is inverse to said permuting function, and an inverse mixing function which is inverse to said mixing function” col. 28, lines 29-38.

It would have been obvious to one of ordinary skill in the art at the time of the invention cryptographic co-processor taught in '871 to include a means to utilize a different cipher function such as invertible key dependent rounds. One of ordinary skill in the art would have been motivated to perform such a modification because stronger flexible algorithms are needed for security see '129 (col. 2, lines 30 et seq.) "After twenty years, many believe that a new stronger, more flexible algorithm is needed. One way to make a cipher stronger is to increase the number of rounds of ciphering performed: with each successive transformation, the resulting encryption becomes more difficult to break. Another way to increase the strength is to increase the size of the key. Since the contents of the key remain secret, increasing the size adds another level of difficulty for anyone trying to deduce what transformations may have been performed on the original data, because they are unlikely to guess the random number combination making up the key. Yet another way to increase algorithm strength is to increase the size of the "block" on which the cipher performs its transformations. A block is the unit of original data processed during one ciphering operation. The larger the block size, the more difficult it becomes for an adversary to construct a dictionary of plaintext and matching ciphertext, for a given key, large enough to pose a threat to the security of the algorithm. Further, different keys can be used for each round, increasing the number of random number combinations that would have to be correctly guessed in order to break the cipher. These keys are referred to herein as "sub-keys".

As to dependent claim 6, "wherein the combination logic performs mixing, permutation and key-dependent substitution in each round" is shown in '129 col. 4, lines 17-34 "the present invention provides a technique, system, and method for implementing a byte-oriented symmetric key block cipher supporting a variable length input key, a variable

length block, and a variable number of rounds, comprising a subprocess for accessing and retrieving values in substitution boxes (s-boxes); a subprocess for generating sub-keys using this input key and these s-boxes; a subprocess for encrypting input data bytes (where these bytes are part of a block, and the block is part of an input data file) using the generated sub-keys and the s-boxes, producing encrypted data bytes (which are part of a corresponding encrypted block, which is part of an encrypted data file); and a subprocess for decrypting the encrypted data bytes using the sub-keys and s-boxes, resulting in restoration of the input data bytes”.

As to dependent claim 7, “wherein the combinational logic enciphers a block by performing an initial permutation of a block to be enciphered and then a complex key-dependent computation followed by a permutation which is an inverse of the initial permutation” is disclosed in ‘129 col. 7, lines 13-26 “The present invention accomplishes encryption of data using the steps of mixing, permutation, and key-dependent substitution for particular, defined groups of bytes of the block of data. A similar approach, with corresponding steps, is used for generating the sub-keys from the key for each round of the cipher. Decryption of data is accomplished in the present invention using the inverse of the data encryption, where the steps are key-dependent inverse substitution, inverse permutation, and inverse mixing. The terms "key-dependent inverse substitution", " inverse permutation", and "inverse mixing" mean that the processing performed in each of these decryption steps is the inverse of the processing performed in the corresponding encryption step. By performing inverse processing, in inverse order, the encrypted data is restored to its original content”.

Art Unit: 2134


As to dependent claim 8, “wherein the combinational logic decipheres a block by performing deciphering using the same key as used to encipher the block in a process that is an inverse of the enciphering process” is taught in ‘129 col. 28, lines 29-38.

Conclusion

9. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Ellen C Tran whose telephone number is (571) 272-3842. The examiner can normally be reached from 6:00 am to 4:00 pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner’s supervisor, Kambiz Zand can be reached on (571) 272-3811. The fax phone number for the organization where this application or proceeding is assigned is (571) 273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).


Ellen Tran
Patent Examiner
Technology Center 2134
20 July 2007